INFORMATION MANAGEMENT ELECTRONIC NEWS LETTER

"Improving Customer Awareness through better Communications"

Vol 2 Issue 1 **October 2000**

Worms in the Workplace:

Across the Center as well as the rest of the Corps, our computers and networks are under increased attacks by viruses and worms. Allot information has been sent out to our customers on computer viruses but very little on Worms. The Worms I writing about are not your garden variety type. This article presents our customers with information on Worms, what they are, and how to protect ourselves against them.

What are Worms? Today's government and commercial networks can appear at times to be very unfriendly to work on. From problems dealing with operating system and software application to the hackers either breaking our systems to spreading viruses. The result many times are corrupted systems and compromised internal platforms. The plague of viruses continues to attract much attention and resources, while proper upkeep and maintenance of virus protection requires constant monitor by our staff.

There is another threat that exists which is less well-understood, and represents an even more dangerous threat to our information and automation resources. Where viruses can spread without manual intervention once introduced within a network a worm can pose a more lethal threat. According to the Microsoft Computer Dictionary, a Worm is a "program that propagates itself across computers, usually by creating copies of itself in each computer's memory." The term originated with the Morris Internet worm of 1988. The Morris worm spread itself from server to server across the Internet, with amazing speed crossing network boundaries.

Anatomy of a Worm: Worms, while often confused with viruses, execute more like a human hacker. Occasionally, that corruption is combined with some repetitive activity, such as was the case with the LoveBug virus, which destroyed audio and graphics files, and also mailed itself to multiple users from the corrupted system's address book. Viruses are also dependent upon some proactive step from the user of the attacked machine. Typically, this will involve executing some questionable content or opening an infected attachment or document.

The migration of the worm from system to system uses much the same process as that used by a well-orchestrated hacking attack, only automated. From the corrupted machine, the worm executes an automated set of tools to probe for weaknesses on the network. Exposed systems with vulnerabilities are identified, and the worm then executes automated attacks against those particular vulnerabilities. Once the target system is compromised, the worm installs itself on the newly corrupted system, and the cycle begins afresh.

A common tactic includes the installation of remote access or communications utilities that allow the author of the worm to have unlimited access to the resources of the affected machine. All of this transpires without significant impact on the attacking machine or the attacked machine, and is often undetected by the affected users or organizations.

The corrupted machines are generally internal servers that share information, and operate as mail systems, file and print servers, source code repositories or departmental infrastructure. From these platforms, all of an organization's private data can be exposed to the prying eyes of the attacker without any need for the attacker to expose himself or herself by manually entering the system.

Prevention of Worm Damage: Two areas of prevention will minimize vulnerability to worm-based attacks: preventing infection and preventing propagation.

Preventing Infection: Preventing worms from being installed can never be a perfect treatment, as there is a natural latency between the time when a system vulnerability or new virus is discovered in the field, and the time when existing preventative measures like virus scanning can take measures against it. However, the likelihood of infection can be minimized through existing well-understood security policies and practices:

- Install and maintain current versions of anti-virus software.
- Prohibit the installation of unauthorized software on systems.
- Practice safe browsing on the Internet. Some content types are vulnerable to exploit, and can be used to load worms onto unknowing systems. The seemingly read-only feel of the Internet experience can lull users into a false sense of security.

INFORMATION MANAGEMENT ELECTRONIC NEWS LETTER

"Improving Customer Awareness through better Communications"

Vol 2 Issue 1 October 2000

- Use a firewall for dedicated home-office Internet connections. Persistent home connections are now common areas in which systems are vulnerable to attack.

With these precautions in place, the likelihood of infection is greatly reduced, and internal networks will be far less vulnerable to the types of worm infestation that we have described.

DITSCAP

DITSCAP: *New Requirements for the Certification and Accreditation (C&A) of all Automated Information Systems (AIS) at Huntsville Center.* By Gary Douglas

The following article is a reprint from an article we ran last year on information security and assurance.
Is the Information Technology you are using at Huntsville Center legal? To be legal, the Certification and Accreditation (C&A) of all Corps of Engineers Information Technology (hardware, software and connective) must now meet the Department Of Defense (DOD) Information Technology Certification & Accreditation Process (DITSCAP) regulation. This will require a complete C&A process be performed for each AIS at Huntsville Center.

The DITSCAP definition of an Automated Information System (AIS) is " Any equipment or interconnected or intra-connected system or subsystem of equipment that is used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes computer software, firmware and hardware". There are Generic and Operational AISs. Generic AIS's are standard CEHQ systems and will be accredited at CEHQ. Operational AIS's are all others and must be accredited at the Organization level. The major definition requirements for each AIS will be :

- A mission description and system identification
- An environment and threat description
- A complete system architecture description
- System security requirements
- Identification of Organizations involved and resources required
- Life Cycle Management documentation
- Contingency Plan (COOP)

The above elements must be collected into a draft System Security Authorization Agreement (SSAA) and registered with the Designated Approving Authority (DAA). The draft document will then go through the process of verification, validation, and post-accreditation. Upon acceptance in the post-accreditation process, Certification and Accreditation for that AIS will be approved.

The single PC user probably will not be affected significantly by this process but systems meeting the DISTCAP AIS definition must be accredited, regardless of the location where they are operational. The approved SSAA document is a living document and will require much work and coordination with many people.

Common Microcomputer Terminology:

CD-ROM (compact disc, read-only memory) drive—A device that reads CD-ROMs. These drives are standard on many PCs and are available in various speeds, which are represented as multiples of X. Most systems presently offer drives averaging 32X or 40X.

CD-RW (compact disc-rewriteable) drive—A CD-based drive that can record or erase data, as well as read it.

CPU (central processing unit)—Think of the CPU, or microprocessor, as the brain of a system. The CPU is a silicon chip that deciphers and initiates your commands. The clock speed of CPUs (recorded in MHz [megahertz], or millions of cycles per second) is a major factor of how fast the microprocessor can perform its calculations.

DVD (digital versatile disc) drive—A drive that can read audio and software CD-ROMs and DVDs, which store up to 4.7GB (gigabytes) of information on each side of the disc.

Ethernet—The most common type of protocol used for LANs (local-area networks). Protocols are sets of standards that spell out the rules for how PCs communicate and exchange data.

GHz (gigahertz)—A measurement used to gauge the speed of a CPU. One GHz is equivalent to 1 billion cycles per second.

hard drive—The main component a computer uses to permanently store and retrieve information. These drives are sealed boxes that are typically found inside the PC case. Today's hard drives have an average storage capacity of 10GB (gigabytes) to more than 20GB.

KB (kilobyte)—An amount of storage equivalent to 1,024 bytes, or approximately 1,000 characters of information.

MB (megabyte)—Also referred to as a meg, a megabyte is a measurement of computer storage that equals 1,048,576 bytes. Bytes are typically represented in computer terminology by an uppercase "B."

MHz (megahertz)—A measurement used to gauge the speed of a CPU (central processing unit). One MHz is equivalent to 1 million cycles per second.

microprocessor—An integrated circuit known as the CPU (central processing unit) that controls the computer.

motherboard—A circuit board inside a computer that provides the foundation for the system. The motherboard holds all the internal circuitry for the system, such as the CPU, buses, memory sockets, expansion slots, etc.

OS (operating system)—Software that handles the computer's basic functions and acts as a foundation to run additional programs. Operating systems recognize keyboard input, send the output to monitors and printers, control peripheral devices, handle system security, and keep records of files and directories. Microsoft Windows 95, Windows 98, and Windows NT are examples of operating systems.

USB (Universal Serial Bus)—An external bus that is expected to eventually replace serial and parallel ports for adding peripherals to a system. Most of today's PCs feature two or more USB ports that provide plug-and-play and hot-swapping capabilities.

Zip drive—A type of storage system designed by Iomega that holds 100MB or 250MB of data on portable diskettes. Zip drives are a popular device used for storing, transporting, and backing up files.

Suggestions

If you would like to make a suggestion on how we can improve our services or would like to make a suggestion on ways to improve this letter please fill out our suggestion form. Click here ✉